that must be submitted to DHS pursuant to a Federal legal requirement, nor do they pertain to any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted to DHS pursuant to the CII Act of 2002). The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information to a Federal agency under any other provision of law. Information submitted to any other Federal agency pursuant to a Federal legal requirement is not to be marked as submitted or protected under the CII Act of 2002 or otherwise afforded the protection of the CII Act of 2002, provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as Protected CII or otherwise afforded the protections of the CII Act of 2002.

(b) *Freedom of Information Act disclosure exemptions.* Information that is separately exempt from disclosure under the Freedom of Information Act or applicable State or local law does not lose its separate exemption protection due to the applicability of these procedures or any failure to follow them.

(c) *Restriction on use of Protected CII by regulatory and other Federal agencies.* No Federal agency shall request, obtain, maintain, or use information protected under the CII Act of 2002 as a substitute for the exercise of its own legal authority to compel access to or submission of that same information. Federal agencies shall not utilize Protected CII for regulatory purposes without the written consent of the submitter or another party on the submitter's behalf.

(d) *Independently obtained information.* These procedures shall not be construed to limit or in any way affect the ability of a Federal, State, or local government entity, agency, or authority, or any third party, under applicable law, to otherwise obtain CII by means of a different law, regulation, rule, or other authority, including such information as is lawfully and customarily disclosed to the public. Independently obtained information does not include any information derived directly or indirectly from Protected CII subsequent to its submission. Nothing in these procedures shall be construed to limit or in any way affect the ability of such entities, agencies, authorities, or third parties to use such information in any manner permitted by law.

(e) *No private right of action.* Nothing contained in these procedures is intended to confer any substantive or procedural right or privilege on any person or entity. Nothing in these procedures shall be construed to create a private right of action for enforcement of any provision of these procedures or a defense to noncompliance with any independently applicable legal obligation.

§ 29.4 Protected Critical Infrastructure Information Program administration.

(a) *IAIP Directorate Program Management.* The Secretary of the Department of Homeland Security hereby designates the Under Secretary of the Information Analysis and Infrastructure Protection (IAIP) Directorate as the senior DHS official responsible for the direction and administration of the Protected CII Program.

(b) *Appointment of a Protected CII Program Manager.* The Under Secretary for IAIP shall:

(1) Appoint a Protected CII Program Manager within the IAIP Directorate who is responsible to the Under Secretary for the administration of the Protected CII Program;

(2) Commit resources necessary to the effective implementation of the Protected CII Program;

(3) Ensure that sufficient personnel, including such detailees or assignees from other Federal national security, homeland security, or law enforcement entities as the Under Secretary deems appropriate, are assigned to the Protected CII Program to facilitate the expeditious and secure sharing with appropriate authorities, including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to

assist in preventing, preempting, or disrupting terrorist threats to our homeland; and

(4) Promulgate implementing directives and prepare training materials as appropriate for the proper treatment of Protected CII.

(c) *Appointment of Protected CII Officers.* The Protected CII Program Manager shall establish procedures to ensure that any DHS component or other Federal, State, or local entity that works with Protected CII appoints one or more employees to serve as a Protected CII Officer for the activity in order to carry out the responsibilities stated in paragraph (d) of this section. Persons appointed to these positions shall be fully familiar with these procedures.

(d) *Responsibilities of Protected CII Officers.* Protected CII Officers shall:

(1) Oversee the handling, use, and storage of Protected CII;

(2) Ensure the expeditious and secure sharing of Protected CII with appropriate authorities, as set forth in § 29.1(a) and paragraph (b)(3) of this section;

(3) Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the entity's handling, use, and storage of Protected CII;

(4) Establish additional procedures as necessary to prevent unauthorized access to Protected CII; and

(5) Ensure prompt and appropriate coordination with the Protected CII Program Manager regarding any request, challenge, or complaint arising out of the implementation of these procedures.

(e) *Protected Critical Infrastructure Information Management System (PCIIMS).* The Protected CII Program Manager or the Protected CII Program Manager's designees shall develop and use an electronic database, to be known as the "Protected Critical Infrastructure Information Management System" (PCIIMS), to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of Protected CII. This compilation of Protected CII shall be safeguarded and protected in accordance with the provisions of the CII Act of 2002.

§ 29.5 Requirements for protection.

(a) CII shall receive the protections of section 214 of the CII Act of 2002 only when:

(1) Such information is voluntarily submitted to the Protected CII Program Manager or the Protected CII Program Manager's designees;

(2) The information is submitted for use by DHS for the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purposes including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland, as evidenced below;

(3) The information is accompanied by an express statement as follows:

(i) In the case of written information or records, through a written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the Federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002"; or

(ii) In the case of oral information, within fifteen calendar days of the oral submission, through a written statement comparable to the one specified above, and a certification as specified below, accompanied by a written or otherwise tangible version of the oral information initially provided; and

(4) The submitted information additionally is accompanied by a statement, signed by the submitting entity, certifying essentially to the following on behalf of the named entity:

(i) The submitter is voluntarily providing the information for the purposes of the CII Act of 2002;

(ii) The information being submitted is not being submitted in lieu of independent compliance with a Federal legal requirement;

(iii) The information is or is not required to be submitted to a Federal agency. If the information is required to be submitted to a Federal agency, the submitter shall identify the Federal agency requiring submission and the legal authority that mandates the submission; and